



Application for a Pierce Network Account

(Revised 08/29/2007)

Please complete ALL sections of the following application and **submit the signed original** to the IT TECH Desk Office located in room C254, Cascade Building, Ft. Steilacoom. If you have any questions about this application, please phone or e-mail the TECH Desk [Tech@pierce.ctc.edu, 253-840-8324].

NEW ACCOUNT

CHANGE TO EXISTING ACCOUNT

NOTE: ALL items are required unless otherwise noted. If not complete, the application will be returned without processing.

Personal Information

Last Name _____, First Name _____ M.I. _____

Work Information

College/ Site location: District Ft. Steilacoom Puyallup
 Ft. Lewis McChord Other _____

Department/Division: _____ Title: _____

Building: _____ Office Room #: _____
(Please provide Division room number if one was not assigned)

Work Phone _____ Fax (Optional): _____
(Please provide the Division or Department phone # if one was not assigned)

Employee Information

Employment Status

- Full Time
- Part Time

Employee Type:

(Note: If selecting either Student employee type, the status will automatically default to Part-Time)

- Classified Exempt (Professional) Faculty
- Administrator Student Intern/Work-study/Volunteer Student Leadership

Account Options

- Pierce College Network / E-Mail Account
- E-Mail Account Forwarding to Personal E-Mail Account – Address: _____
(Note: Checking this box will cause **all** Pierce College E-Mail to be forwarded to your personal E-Mail account!)

I hereby request a Pierce College District Network account for purposes of accessing the District network, e-mail, and the Internet. I agree to abide by the policies, procedures and guidelines of the District, the K-20 Network, and the Washington State Executive Ethics Board regarding use of this account. I further acknowledge my responsibility to read, understand and agree to abide by the Pierce College District and K-20 policies, procedures and guidelines. **Note:** You can access these policies and associated procedures/guidelines via the Internet at the following links (you can use the computers in the Pierce College Libraries if you don't yet have an account):

Washington State Executive Ethics Board Manual: <http://ethics.wa.gov/TRAINING/2007%20training%20manual%20revised.htm>

K-20 Network Conditions of Use and Acceptable Use Policies: http://www.wa-k20.net/docs/K-20_AUP.doc

Pierce College Acceptable Use Policy: <http://www.pierce.ctc.edu/policy/policyCh1.htm#1.22.0000>

Pierce College Acceptable Use Procedure: <http://www.pierce.ctc.edu/policy/procedures/CISR-AcceptableUse.pdf>

Pierce College Limited Personal Use Policy: <http://www.pierce.ctc.edu/policy/policyCh1.htm#1.22.0001>

By signing below, I am verifying I have read the Pierce College District and K-20 Acceptable Use policies, procedures and guidelines, and the Executive Ethics Board guidelines for computer related use. I agree to abide by their provisions.

Employee Signature _____ Date _____

Supervisor of Record/Area Administrator Name (printed) _____

Supervisor of Record/Area Administrator Signature _____ Date _____

[Employee **AND** Supervisor of Record or Area Administrator signatures are required for **ALL** accounts.]

FOR IT USE ONLY

Account Creation Date _____ Account Creator _____

USERNAME _____ Notification Date _____

Using a secure password is your responsibility. A password compromised on a single user's account can jeopardize system security for all other users on the server and potentially remote network sites as well. As a result, we rely on every user to take password security seriously. Software programs exist that can generate variations of common names and words in an attempt to "crack" your password.

Running "password cracking" programs is a serious security offense, and may be subject to legal action here and at other institutions. Unfortunately, however, these programs are relatively easy to obtain and difficult to trace. The best protection is to be aware of the criteria used by these programs, and to carefully follow the guidelines below. Unfortunately, the negative precautions far outnumber the positive, so be sure to read the final section offering examples of secure passwords.

General Password Guidelines

1. Never share your password with anyone - including family, friends, or colleagues. Although this may sound draconian, there are at least 3 justifications:
 - A. Sharing of accounts is not permitted on the District networks or servers.
 - B. The responsibility to protect your password cannot be shared or transferred to anyone else.
 - C. By sharing your password with a confidant, you create the potential that sanctions may be brought against him/her for violating rule (A).
2. Never write down your password -- unless you intend to keep it in a secure, locked in a place only accessible by you. NOTE: Office desk drawers and file cabinets usually do NOT meet these criteria, unless the password is kept in a sealed, safety envelope.
3. Periodically change your password.
4. Never use a password suggested by someone else, either in person, by phone, or through electronic mail.
5. Do not use any specific sample password listed in this memo.

What to Avoid When Choosing a Password

1. Do not choose any proper name, nickname, or part of a name.
2. Do not use an unbroken sequence of numbers, such as "3840183".
3. Do not use any single real word in the dictionary as the basis for your password. All of the following are easily "guessed" by password cracking programs:
 - A. Syntactic variant of a word: **answer --> answered, answering, answers**
 - B. Adding digits, blank spaces, mixed case, or other "characters" to a word: **gre123en, hel.Los, aNdr&A**
 - C. Reversing, "reflecting", or doubling a word: **yadiloh, fredderf, samesame**
 - D. Stripping vowels from a word: **Mississippi --> msssspp**
 - F. Substituting digits or characters for letters they resemble:
i or l --> 1
Do --> D0
4s --> 4\$

Tips on Choosing a More Secure Password

1. Select a password that is 6-10 characters long.
2. Use a combination of upper/lower case, numbers, and "special characters" on keyboard.
Special Characters: { } [] , . < > ; : ' " ? / \ ` ~ ! @ # \$ % ^ & * () _ - + =
2. Combine more than one (unrelated) word or name to form the basis of your password and then add a number: **Salt2~try, tan_7West, no\$CAndo8**
3. Select meaningless words that are "easy" to remember: **1Form.dot, tar-Windo5**
4. Distort spelling of real words: **2;pattirN, sytuRn)5, doarMat3[**

[Please print and keep this page for reference]